Discrete Mathematics 125 (1994) 263–272
North-Holland

On subsets of partial difference sets

S.L. Ma

Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 0511, Singapore

Received 12 July 1991
Revised 31 October 1991

Abstract

Let G be a finite group of order v. A k-element subset D of G is called a (v, k, λ, μ)-partial difference set in G if the expressions gh^{-1}, for g and h in D with $g \neq h$, represent each nonidentity element contained in D exactly λ times and represent each nonidentity element not contained in D exactly μ times. Suppose G is abelian and H is a subgroup of G such that $\gcd(|H|, |G|/|H|) = 1$ and $|G|/|H|$ is odd. In this paper, we show that if D is a partial difference set in G with $\{d^{-1} | d \in D\} = D$, then $D \cap H$ is a partial difference set in H.

1. Introduction

Let G be a finite group of order v. A k-element subset D of G is called a (v, k, λ, μ)-*partial difference set* (or briefly *PDS*) in G if the expressions gh^{-1}, for g and h in D with $g \neq h$, represent each nonidentity element contained in D exactly λ times and represent each nonidentity element not contained in D exactly μ times. (Note that the parameters defined above are different from those in [5, 6]. A (v, k, α, β)-partial difference set defined in [5, 6] is, according to our definition, a $(v, k, \alpha+\beta, \alpha)$-partial difference set, i.e. $\lambda = \alpha + \beta$ and $\mu = \alpha$.)

For an integer t, we define $D^{(t)} := \{g^t | g \in D\}$. From [5], we learn that if D is a (v, k, λ, μ)-PDS with $\lambda \neq \mu$, then $D^{(-1)} = D$. The case $\lambda = \mu$ means that D is just an ordinary difference set and a lot of work has been done on this topic (see [1, 4]). Thus, here, it is natural for us to concentrate on the case $\lambda \neq \mu$, or generally, $D^{(-1)} = D$. Note that a PDS D with $D^{(-1)} = D$ and $1 \notin D$, where 1 is the identity element in G, is equivalent to a strongly regular graph which admits a regular automorphism group (see [2, 6]).

Usually, the study of difference sets is carried out using the group ring $\mathbb{Z}[G]$ or $\mathbb{C}[G]$. For $S \subset G$, let $\bar{S} := \sum_{g \in S} g$. Then a subset D in G is a (v, k, λ, μ)-PDS if and only if

$$\bar{D}\bar{D}^{(-1)} = \mu\bar{G} + (\lambda - \mu)\bar{D} + \gamma, \tag{1.1}$$

Correspondence to: S.L. Ma, Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 0511, Singapore.

SSDI 0012-365X(92)00204-2

where $\gamma := k-\mu$ if $1 \notin D$ and $\gamma := k-\lambda$ if $1 \in D$. Furthermore, if $D^{(-1)}=D$, then $\bar{D}^2 = \mu\bar{G}+(\lambda-\mu)\bar{D}+\gamma$ and

$$(2\bar{D}-\beta)^2 = 4\mu\bar{G}+\Delta, \tag{1.2}$$

where $\beta := \lambda-\mu$ and $\Delta := (\lambda-\mu)^2+4\gamma$. Note that β and Δ are very useful parameters in classifying PDSs.

Definition 1.1. (a) A PDS D with parameters as described above is called a *PDS of type* (β, Δ).

(b) A PDS D in G is called *trivial* if $D \cup \{1\}$ or $(G\backslash D)\cup\{1\}$ is a subgroup of G. Otherwise, D is called *nontrivial*.

(c) A subset D of G is called *reversible* if $D^{(-1)}=D$.

Note that, for any m, $\emptyset, \{1\}, G\backslash\{1\}$ and G are PDSs in G of type $(\pm m, m^2), (\pm m+2, m^2), (\pm m-2, m^2)$ and $(\pm m, m^2)$, respectively. Also, if N is a subgroup of order w in G, then $G\backslash N, (G\backslash N)\cup\{1\}, N\backslash\{1\}$ and N are PDSs in G of type $(-w, w^2), (-w+2, w^2), (w-2, w^2)$ and (w, w^2), respectively.

Proposition 1.2. *Let D be a reversible PDS of type (β, Δ) in G. Then*

(i) *β and Δ have the same parity,*

(ii) *if $1 \notin D$, then D is nontrivial if and only if $-\sqrt{\Delta} < \beta < \sqrt{\Delta}-2$; if $1 \in D$, then D is nontrivial if and only if $-\sqrt{\Delta}+2 < \beta < \sqrt{\Delta}$.*

Proof. By comparing the coefficients of the identity in (1.2), we have $4k+\beta^2 = 4\mu+\Delta$ if $1 \notin D$ and $4(k-1)+(\beta-2)^2 = 4\mu+\Delta$ if $1 \in D$. Thus, β and Δ must have the same parity.

For (ii), if $1 \in D$, then $D\backslash\{1\}$ is a PDS of type $(\beta-2, \Delta)$. Hence, we only need to prove the statement in the case $1 \notin D$. If D is trivial, then $\beta = \pm\sqrt{\Delta}$ or $\pm\sqrt{\Delta}-2$. Suppose D is nontrivial. Since $k \geqslant \mu$, we have $-\sqrt{\Delta} \leqslant \beta \leqslant \sqrt{\Delta}$. We shall show that $\beta \neq \pm\sqrt{\Delta}$ and $\sqrt{\Delta}-2$.

Suppose $\beta^2 = \Delta$. Then $\gamma = 0$ and $k = \mu$. By counting the number of elements on both sides of (1.1), we have $k^2 = kv+\beta k$; hence, $k=0$ or $v+\beta$. If $k=0$, then $D=\emptyset$. For $k = v+\beta$, let $D_1 = G\backslash D$. Note that $\bar{D}_1\bar{D}_1^{(-1)} = -\beta\bar{D}_1$. This implies D_1 is a subgroup of G.

For $\beta = \sqrt{\Delta}-2$, a similar result can be obtained by considering $(G\backslash D)\backslash\{1\}$. □

Theorem 1.3 (Ma [5, Corollary 5.5]). *If there exists a (v, k, λ, μ)-reversible PDS of type (β, Δ) in an abelian group such that Δ is not a square, then*

$$(v, k, \lambda, \mu, \beta, \Delta) = \begin{cases} (p^{2s+1}, \frac{1}{2}(p^{2s+1}-1), \frac{1}{4}(p^{2s+1}-5), \frac{1}{4}(p^{2s+1}-1), -1, p^{2s+1}) \\ \qquad\qquad \text{if } 1 \notin D \\ (p^{2s+1}, \frac{1}{2}(p^{2s+1}+1), \frac{1}{4}(p^{2s+1}+3), \frac{1}{4}(p^{2s+1}-1), -1, 1, p^{2s+1}) \\ \qquad\qquad \text{if } 1 \in D \end{cases}$$

where p is a prime such that $p \equiv 1 \bmod 4$.

Theorem 1.4 (Ma [5, Theorem 4.1]). *Let D be a reversible PDS of type (β, Δ) in an abelian group G. If t is any integer relatively prime to the order of G, then $D^{(t^2)}=D$. Furthermore, if Δ is a square, then $D^{(t)}=D$.*

2. The dual of a partial difference set

From now on, we always assume that G is an abelian group of order v and D is a reversible PDS of type (β, Δ) in G with $|D|=k$. Let G^* be the group of characters of G. For $\chi \in G^* \setminus \{1\}$, by (1.2), we have $\chi \bar{D}=(\beta \pm \sqrt{\Delta})/2$. (For convenience, 1 is also used as the identity element in G^*.)

Definition 2.1. If $D \neq \emptyset, \{1\}, G\setminus\{1\}$ and G, then we define

$$D^+ := \{\chi \in G^* \setminus \{1\} \mid \chi \bar{D}=(\beta+\sqrt{\Delta})/2\},$$

which is called the *dual* of D.

The following is a well-known theorem on the dual of a PDS (see [2, 3, 5]).

Theorem 2.2. *If $1 \notin D$ and $D \neq \emptyset, G\setminus\{1\}$, then D^+ is a reversible PDS of type (β^+, Δ^+) in G^* where $\beta^+ := (v-2k+\beta-\sqrt{\Delta})/\sqrt{\Delta}$ and $\Delta^+ := v^2/\Delta$. Also, $k^+ := |D^+| = [(\sqrt{\Delta}-\beta)(v-1)-2k]/2\sqrt{\Delta}$.*

Note that if $1 \in D$, then $D^+ = (D\setminus\{1\})^+$. Hence, D^+ is a reversible PDS and the parameters can be computed by replacing k and β by $k-1$ and $\beta-2$, respectively, in Theorem 2.2.

Corollary 2.3. *If $1 \notin D$ and $D \neq \emptyset, G\setminus\{1\}$, then*

$$\left(2\bar{D}^+ - \frac{v-2k+\beta-\sqrt{\Delta}}{\sqrt{\Delta}}\right)^2 = \frac{v}{\Delta}[(\sqrt{\Delta}-\beta-1)^2-1]\bar{G}^* + \frac{v^2}{\Delta}. \tag{2.1}$$

Proposition 2.4. *If $1 \notin D$ and $D \neq \emptyset, G\setminus\{1\}$, then:*

(i) $v^2 \equiv (2k-\beta)^2 \equiv (\beta^2+2\beta)v \equiv 0 \bmod \Delta$,

(ii) *if D is nontrivial, then v and Δ have the same prime divisors.*

Proof. If Δ is not a square, then the proposition follows from Theorem 1.3. Suppose $\Delta=\delta^2$ where δ is an integer. Then $v \equiv 2k-\beta \equiv 0 \bmod \delta$ because Δ^+ and β^+ in Theorem 2.2 are integers. Also, $(\beta^2+2\beta)v \equiv 0 \bmod \delta^2$ since $(v/\delta^2)[(\delta-\beta-1)^2-1]$ in (2.1) is an integer. Finally, (ii) follows from $\delta | v$ and [5, Theorem 6.2]. □

For any $g \in G$, we define X_g to be a character of G^* such that $X_g(\chi)=\chi g$ for all $\chi \in G^*$. Note that $\sigma : g \mapsto X_g$ is a one-to-one correspondence between G and $(G^*)^*$, the group of characters of G^*.

Theorem 2.5. *If* $1 \notin D$ *and* $D \neq \emptyset, G \setminus \{1\}$, *then* $\sigma^{-1}[(D^+)^+] = D$.

Proof. The theorem follows from the Fourier inversion formula (see [8, Chap. 7]), and $D^{(-1)} = D$. □

3. The main result

Recall that G is an abelian group of order v. Let p be an odd prime divisor of v such that $v = p^t w$ where w is relatively prime to p. Let P be the Sylow p-subgroup of G and H be a subgroup of G of order w. Note that G is a direct product of P and H.

Let $Q := D \cap H$ where D is a nontrivial reversible PDS of type (β, Δ) in G with $1 \notin D$. Without loss of generality, we may assume that Δ is a square, say $\Delta = \delta^2$ where δ is a positive integer. (Note that if Δ is not a square, then $v = p^t$; hence, $P = G$ and $H = \{1\}$.) In this section, we show that Q is a reversible PDS in H.

We need two lemmas from [7].

Lemma 3.1 (Ma [7, Lemma 2.2]). *Let* N *be a finite abelian group and* $y \in \mathbb{Z}[N]$. *Let* p *be a prime such that* $p \nmid |N|$. *If* $\chi y \equiv 0 \bmod p^s$ *for all characters* χ *of* N, *then* $y = p^s x$ *for some* $x \in \mathbb{Z}[N]$.

Lemma 3.2 (Ma [7, Lemma 2.3]). *Let* $X_i, i = 1, 2, \ldots, \theta + \varphi$, *be integers such that* X_i *is odd when* $1 \leqslant i \leqslant \theta$, X_i *is even when* $\theta + 1 \leqslant i \leqslant \theta + \varphi$ *and* $\sum_{i=1}^{\theta+\varphi} X_i = L$. *Then*

$$\sum_{i=1}^{\theta+\varphi} X_i^2 \geqslant \frac{L^2 + \theta\varphi}{\theta + \varphi}$$

and equality holds if and only if either

(i) $X_i = (L + \varphi)/(\theta + \varphi)$ *when* $1 \leqslant i \leqslant \theta$ *and* $X_i = (L - \theta)/(\theta + \varphi)$ *when* $\theta + 1 \leqslant i \leqslant \theta + \varphi$ *or*

(ii) $X_i = (L - \varphi)/(\theta + \varphi)$ *when* $1 \leqslant i \leqslant \theta$ *and* $X_i = (L + \theta)/(\theta + \varphi)$ *when* $\theta + 1 \leqslant i \leqslant \theta + \varphi$.

Suppose $\delta = p^r \pi$ where π is relatively prime to p. Let $H^\perp := \{\chi \in G^* \mid \chi \text{ is principal on } H\}$ and $P^\perp := \{\chi \in G^* \mid \chi \text{ is principal on } P\}$. Note that $|H^\perp| = p^t$, $|P^\perp| = w$ and G^* is a direct product of $H^\perp$ and $P^\perp$. Let $\rho : G^* \to P^\perp$ be the projection which maps all elements in $H^\perp$ onto the identity. By (2.1), we have

$$\rho\left(2\bar{D}^+ - \frac{v - 2k + \beta - \delta}{\delta}\right)^2 = \frac{w}{\pi^2} p^{2t-2r}[(\delta - \beta - 1)^2 - 1]\bar{P}^\perp + \frac{w^2}{\pi^2} p^{2t-2r}.$$

Let X be a character of $P^\perp$. Then

$$X\rho\left(2\bar{D}^+ - \frac{v - 2k + \beta - \delta}{\delta}\right) = \begin{cases} \pm\dfrac{w}{\pi} p^{t-r} & \text{if } X \text{ is not principal on } P^\perp, \\ \dfrac{w}{\pi}(\delta - \beta - 1) p^{t-r} & \text{if } X \text{ is principal on } P^\perp, \end{cases}$$
$$\equiv 0 \bmod p^{t-r}.$$

By Lemma 3.1,

$$z := \frac{1}{p^{t-r}}\rho\left(2\bar{D}^+ - \frac{v-2k+\beta-\delta}{\delta}\right)$$

has integral coefficients. Note that

$$z^2 = \frac{w}{\pi^2}[(\delta-\beta-1)^2-1]\bar{P}^\perp + \frac{w^2}{\pi^2}. \tag{3.1}$$

Let $R := D^+ \cap P^\perp$ and, for $\chi \in P^\perp$, e_χ be the coefficient of χ in z.

Lemma 3.3. (i) $e_1 = (\delta-\beta-w+2|Q|)/\pi$ *and* $\sum_{\chi\neq 1} e_\chi = [(\delta-\beta)(w-1)-2|Q|]/\pi$.
(ii) *For* $\chi \in P^\perp \setminus \{1\}$, $e_\chi \equiv 0 \bmod 4$ *if* $\chi \notin R$; $e_\chi \equiv 2 \bmod 4$ *if* $\chi \in R$.

Proof. Let $Q^* := D^+ \cap H^\perp$, P^* be the group of characters of P and $\rho_1 : G \to P$ be the projection from G to P which maps all elements of H onto the identity. Then by the Fourier inversion formula (see [8, Chap. 7]),

$$\begin{aligned}
|Q| &= |D \cap H| \\
&= \text{the coefficient of the identity in } \rho_1 \bar{D} \\
&= \frac{1}{|P|}\sum_{\chi\in P^*} \chi(\rho_1 \bar{D}) \\
&= \frac{1}{|P|}\sum_{\chi\in H^\perp} \chi \bar{D} \\
&= \frac{1}{p^t}\left[k + \left(\frac{\beta+\delta}{2}\right)|Q^*| + \left(\frac{\beta-\delta}{2}\right)(p^t - |Q^*| - 1)\right];
\end{aligned}$$

hence,

$$|Q^*| = \frac{1}{2\delta}[2p^t|Q| - 2k - (\beta-\delta)(p^t-1)].$$

Thus, (i) follows since

$$e_1 = \frac{1}{p^{t-r}}\left(2|Q^*| - \frac{v-2k+\beta-\delta}{\delta}\right) \quad \text{and} \quad \sum_{\chi\neq 1} e_\chi = \frac{2}{p^{t-r}}(|D^+| - |Q^*|).$$

Let $\tau\chi \in D^+$ with $\tau \in H^\perp$ and $\chi \in P^\perp \setminus \{1\}$. For any t relatively prime to p, we can choose an integer t' relatively prime to v such that $t' \equiv t \bmod |H^\perp|$ and $t' \equiv 1 \bmod |P^\perp|$. By Theorem 1.4, we have $D^{+(t')} = D^+$; consequently, $\tau^t\chi \in D^+$. Thus,

$$C(\tau, \chi) := \{\tau^t\chi \mid t \text{ is relatively prime to } p\} \subset D^+.$$

Note that

$$|C(\tau,\chi)|=\begin{cases}p^{s-1}(p-1) & \text{if } o(\tau)=p^s \text{ for } s>0,\\ 1 & \text{if } \tau=1.\end{cases}$$

The coefficient of χ in $\rho\bar{D}^+$ is equal to

$$|H^\perp\chi\cap D^+|=\left|\bigcup_{\tau\in(H^\perp\chi\cap D^+)\chi^{-1}} C(\tau,\chi)\right| \equiv\begin{cases}0 \bmod (p-1) & \text{if } \chi\notin R,\\ 1 \bmod (p-1) & \text{if } \chi\in R.\end{cases}$$

Then (ii) follows since

$$e_\chi=\frac{2}{p^{t-r}}(\text{the coefficient of } \chi \text{ in } \rho\bar{D}^+)$$

and p is *odd*. □

Lemma 3.4.

(i) $\frac{1}{\pi}[|Q|^2-(w-1)|Q|]\leqslant\frac{1}{w/\pi}[|R|^2-(w-1)|R|]$.

(ii) *Equality in* (i) *holds if and only if*

$$z=\left(\frac{\Lambda\mp 2|R|}{w-1}\right)\bar{P}^\perp\pm 2\bar{R}+d, \tag{3.2}$$

where

$$\Lambda:=\sum_{\chi\neq 1} e_\chi \quad \text{and} \quad d:=e_1+\left(\frac{\Lambda\mp 2|R|}{w-1}\right).$$

Proof. By calculating the coefficient of the identity element in (3.1), we have

$$\sum_{\chi\in P^\perp} e_\chi^2=\frac{w}{\pi^2}[(\delta-\beta-1)^2-1]+\frac{w^2}{\pi^2}.$$

On the other hand, by Lemmas 3.2 and 3.3(ii), we have

$$\sum_{\chi\in P^\perp} e_\chi^2=e_1^2+\sum_{\chi\neq 1} e_\chi^2\geqslant e_1^2+\frac{\Lambda^2+4|R|(w-1-|R|)}{w-1}.$$

Equality holds if and only if z satisfies equation (3.2). Hence, the statement follows from Lemma 3.3(i). □

Theorem 3.5. *Q and R are reversible PDSs in H and $P^\perp$, respectively. Furthermore,*

(a) *if $R=\emptyset$ or $P^\perp\backslash\{1\}$, then $Q=\emptyset$ or $H\backslash\{1\}$ and $z=(\Lambda/(w-1))\bar{P}^\perp+d$ and*

(b) *if $R\neq\emptyset$ and $P^\perp\backslash\{1\}$, then, by regarding $P^\perp$ as the group of characters of H, we have either*

$$Q^+=R \quad \text{and} \quad z=\left(\frac{\Lambda-2|R|}{w-1}\right)\bar{P}^\perp+2\bar{R}+d$$

or

$$Q^+ = P^\perp \backslash (R \cup \{1\}) \quad \textit{and} \quad z = \left(\frac{\Lambda + 2|R|}{w-1} \right) \bar{P}^\perp - 2\bar{R} + d.$$

Proof. By applying Lemma 3.4(i) to $S := (D^+)^+ \cap (H^\perp)^\perp$, we have

$$\frac{1}{w/\pi}[|R|^2 - (w-1)|R|] \leqslant \frac{1}{\pi}[|S|^2 - (w-1)|S|].$$

Note that π is replaced by w/π because $\sqrt{\Delta^{\mp}} = v/\delta = p^{t-r}w/\pi$. By Theorem 2.5, $|S| = |Q|$. Thus, equality holds in Lemma 3.4(i). If $R = \emptyset$ or $P^\perp \backslash \{1\}$, then $z = (\Lambda/(w-1))\bar{P}^\perp + d$ follows from (3.2). Also, the equality in Lemma 3.4(i) implies $Q = \emptyset$ or $H \backslash \{1\}$.

Suppose $R \neq \emptyset$ and $P^\perp \backslash \{1\}$. By substituting $z = ((\Lambda \mp 2|R|)/(w-1))\bar{P}^\perp \pm 2\bar{R} + d$ into (3.1), we have $[2\bar{R} \pm d]^2 = a\bar{P}^\perp + (w^2/\pi^2)$ for some integer a. Hence, R is a reversible PDS of type $(\pm d, w^2/\pi^2)$.

Suppose $z = ((\Lambda - 2|R|)/(w-1))\bar{P}^\perp + 2\bar{R} + d$. For any $X \in (H^\perp)^\perp \backslash \{1\}$, it is obvious that $X\bar{R} = (-d + (w/\pi))/2$ if and only if $X\bar{D}^+ = (\beta^+ + (v/\delta))/2$. Therefore, $R^+ = S$ and $(R^+)^+ = S^+$. By Theorem 2.5, we have $R = Q^+$.

Similarly, if $z = ((\Lambda + 2|R|)/(w-1))\bar{P}^\perp - 2\bar{R} + d$, then $X\bar{R} = (d - (w/\pi))/2$ if and only if $X\bar{D}^+ = (\beta^+ + (v/\delta))/2$ for any $X \in (H^\perp)^\perp \backslash \{1\}$. Thus, it follows that $Q^+ = P^\perp \backslash (R \cup \{1\})$. □

Let θ be an integer such that $(2\theta - 1)\pi \leqslant \beta < (2\theta + 1)\pi$. Note that if $Q \neq \emptyset, H \backslash \{1\}$, i.e. $1 \leqslant |Q| \leqslant w-2$, then

$$\left\lfloor \frac{\Lambda}{2(w-1)} \right\rfloor = \left\lfloor \frac{\delta - \beta}{2\pi} - \frac{|Q|}{\pi(w-1)} \right\rfloor = \frac{p^r - 1}{2} - \theta,$$

where $\lfloor c \rfloor$ denotes the greatest integer less than or equal to c.

Theorem 3.6. *Q is of type $(\beta - 2\theta\pi, \pi^2)$.*

Proof. If $Q = \emptyset$, then $R = \emptyset$ or $P^\perp \backslash \{1\}$ and $z = (\Lambda/(w-1))\bar{P}^\perp + d$. Note that $\frac{1}{2}(\Lambda/(w-1)) = (p^r\pi - \beta)/2\pi$ is an integer. So $\beta = (2\theta - 1)\pi$ and it is clear that the empty set is a PDS of type $(-\pi, \pi^2)$ for any π.

Similarly, for $Q = H \backslash \{1\}$, we have $z = (\Lambda/(w-1))\bar{P}^\perp + d$. Now,

$$\frac{1}{2}\left(\frac{\Lambda}{w-1} \right) = \frac{p^r\pi - \beta - 2}{2\pi}$$

is an integer. So $\beta = (2\theta + 1)\pi - 2$ and it is obvious that $H \backslash \{1\}$ is of type $(\pi - 2, \pi^2)$ for any π.

For $Q \neq \emptyset$ and $H \backslash \{1\}$, by Theorem 3.5(b) and R being a reversible PDS of type $(\pm d, w^2/\pi^2)$, Q is a partial reversible PDS of type (β', π^2) for some integer β'. By Theorem 2.5, two cases are to be considered.

Case 1: $Q^+ = R$. We have

$$z = \left(\frac{\Lambda - 2|R|}{w-1}\right)(\bar{P}^\perp - \bar{R} - 1) + \left(\frac{\Lambda - 2|R|}{w-1} + 2\right)\bar{R} + e_1.$$

Thus,

$$\frac{1}{2}\left(\frac{\Lambda - 2|R|}{w-1}\right) = \left\lfloor \frac{\Lambda}{2(w-1)} \right\rfloor = \frac{p^r - 1}{2} - \theta,$$

which implies

$$|Q| + \pi|R| = \tfrac{1}{2}[(2\theta+1)\pi - \beta](w-1).$$

On the other hand, by Theorem 2.2, we have $|Q| + \pi|R| = \frac{1}{2}(\pi - \beta')(w-1)$. So $\beta' = \beta - 2\theta\pi$.

Case 2: $Q^+ = H \setminus (R \cup \{1\})$. We have

$$z = \left(\frac{\Lambda + 2|R|}{w-1}\right)(\bar{P}^\perp - \bar{R} - 1) + \left(\frac{\Lambda + 2|R|}{w-1} - 2\right)\bar{R} + e_1.$$

Thus,

$$\frac{1}{2}\left(\frac{\Lambda + 2|R|}{w-1} - 2\right) = \left\lfloor \frac{\Lambda}{2(w-1)} \right\rfloor = \frac{p^r - 1}{2} - \theta,$$

which implies

$$|Q| - \pi|R| = \tfrac{1}{2}[(2\theta-1)\pi - \beta](w-1).$$

On the other hand, by Theorem 2.2, $|Q| - \pi|R| = \frac{1}{2}(-\pi - \beta')(w-1)$. So $\beta' = \beta - 2\theta\pi$. □

4. Some nonexistence results

By repeatedly applying the results in Section 3, we obtain the following theorem.

Theorem 4.1. *Suppose there exists a nontrivial reversible PDS D of type (β, δ^2) in an abelian group G with $1 \notin D$. If H is a subgroup of G such that $\gcd(|H|, |G|/|H|) = 1$ and $|G|/|H|$ is odd, then $D \cap H$ is a reversible PDS of type $(\beta - 2\theta\pi, \pi^2)$ in H where $\pi := \gcd(|H|, \delta)$ and θ is the unique integer such that $(2\theta-1)\pi \leqslant \beta < (2\theta+1)\pi$.*

Corollary 4.2. *Suppose H be a subgroup of an abelian group G such that $\gcd(|H|, |G|/|H|) = 1$ and $|G|/|H|$ is odd. Let π be a divisor of $|H|$ and $-\pi \leqslant \beta' \leqslant \pi - 2$. If no reversible PDS Q of type (β', π^2) exists in H with $1 \notin Q$, then no reversible PDS D of type $(\beta' + 2\theta\pi, \pi^2 u^2)$ exists in G with $1 \notin D$ where u is any divisor of $|G|/|H|$ and θ is any integer such that $-\pi u < \beta' + 2\theta\pi < \pi u - 2$.*

Note that a reversible difference set of order $n (= k - \lambda)$ is a reversible PDS of type $(0, 4n)$.

Corollary 4.3 (Ma [7, Theorem 3.1]). *Suppose there exists a nontrivial difference set of order n in an abelian group G with -1 as a multiplier. If H is a subgroup of G such that $gcd(|H|, |G|/|H|)=1$ and $|H|$ is even, then there exists a difference set of order n' in H with -1 as a multiplier where $n' := gcd(|H|^2, n)$.*

The following is another theorem obtained from the results in Section 3. This theorem can be regarded as a generalization of a result by McFarland [9, Theorem 3.4] on certain difference sets with -1 as a multiplier.

Theorem 4.4. *Let $\delta = p^r\pi$, where $p \geqslant 5$ is a prime, $\pi > 1$ is relatively prime to p, and β be an integer such that $(2\theta-1)\pi \leqslant \beta < (2\theta+1)\pi$. Suppose there is a nontrivial reversible PDS D of type (β, δ^2) in an abelian group with $1 \notin D$. If $D \cap H \neq \emptyset$ and $H\backslash\{1\}$, then either*

(i) *r is even and $\theta \equiv 0 \bmod (p-1)$ or*

(ii) *r is odd and $\theta \equiv (p-1)/2 \bmod (p-1)$.*

Proof. In the following, we use the notation introduced in Section 3. Let

$$\bar{D}^+ = \sum_{\chi \in P^\perp} \bar{A}_\chi \chi \text{ where } A_\chi := (H^\perp \chi \cap D^+)\chi^{-1} \subset H^\perp.$$

From the proof of Lemma 3.3, it follows that

$$|A_\chi| \equiv \begin{cases} 0 \bmod (p-1) & \text{if } \chi \notin R, \\ 1 \bmod (p-1) & \text{if } \chi \in R. \end{cases} \tag{4.1}$$

Let $\rho: G^* \to P^\perp$ be the projection as defined in Section 3. Then $\rho\bar{D}^+ = \sum_{\chi \in P^\perp} |A_\chi| \chi$. By the proof of Theorem 3.6, we have

$$\begin{aligned} &\frac{1}{p^{t-r}} \rho\left(2\bar{D}^+ - \frac{v-2k+\beta-\delta}{\delta}\right) \\ &\quad = (p^r \mp 1 - 2\theta)(\bar{P}^\perp - \bar{R} - 1) + (p^r \pm 1 - 2\theta)\bar{R} + e_1. \end{aligned} \tag{4.2}$$

Since $Q \neq \emptyset$ and $H\backslash\{1\}$, we have $R \neq \emptyset$ and $P^\perp\backslash\{1\}$. By (4.1) and (4.2), either

$$p^{t-r}\left(\frac{p^r-1}{2} - \theta\right) \equiv 0 \bmod (p-1) \text{ and } p^{t-r}\left(\frac{p^r+1}{2} - \theta\right) \equiv 1 \bmod (p-1)$$

or

$$p^{t-r}\left(\frac{p^r+1}{2} - \theta\right) \equiv 0 \bmod (p-1) \text{ and } p^{t-r}\left(\frac{p^r-1}{2} - \theta\right) \equiv 1 \bmod (p-1).$$

If $p > 3$, then (b) is impossible. □

Note that, in Theorem 4.4, if $(2\theta-1)\pi < \beta < (2\theta+1)\pi - 2$, then $D \cap H \neq \emptyset$ and $H\backslash\{1\}$.

References

[1] T. Beth, D. Jungnickel and H. Lenz, Design Theory (Cambridge Univ. Press, Cambridge, 1986).
[2] W.G. Bridges and R.A. Mena, Rational G-matrices with rational eigenvalues, J. Combin. Theory Ser. A 32 (1982) 264–280.
[3] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Reports Suppl. 10 (1973).
[4] E.S. Lander, Symmetric Designs:An Algebraic Approach (Cambridge Univ. Press, Cambridge, 1983).
[5] S.L. Ma, Partial difference sets, Discrete Math. 52 (1984) 75–89.
[6] S.L. Ma, On association schemes, Schur rings, strongly regular graphs and partial difference sets, Ars Combin. 27 (1989) 211–220.
[7] S.L. Ma, McFarland's conjecture on abelian difference sets with multiplier -1, designs, codes and cryptography, 1 (1992) 321–332.
[8] H.B. Mann, Addition Theorems (Wiley, New York, 1965).
[9] R.L. McFarland, Sub-difference sets of Hadamard difference sets, J. Combin. Theory Ser. A 54 (1990) 112–122.